IN THE CLAIMS:

1. *(currently amended)* A method ~~of authenticating a user of a second system where the user has an authenticated identity in a first system,~~ comprising ~~the steps of~~:

having an identity authenticated in a first system;

~~the second system~~ a second system causing a key to be generated for use in the second system;

the second system generating a certificate for the key; and

establishing the identity of the user in the second system by signing the certificate for the key using the authenticated identity of the user in the first system.

2. *(original)* A method as defined in claim 1, wherein the key is generated by the second system.

3. *(original)* A method as defined in claim 1, wherein the key is generated by the first system.

4. *(original)* A method as defined in claim 1, further comprising the step of: a third party communicating with the user of the second system and verifying the user of the second system by the authenticated identity of the user of the first system.

5. *(original)* A method as defined in claim 4, wherein the third party is a server.

6. *(original)* A method as defined in claim 4, wherein the key comprises a private-public key pair and where the certificate includes the public key of the key pair.

7. *(original)* A method as defined in claim 6, wherein the certificate further includes an identity which is the same as the authenticated identity of the user of the first system.

8. *(original)* A method as defined in claim 7, where the authenticated identity of the user in the first system comprises a private-public key pair and a certificate issued by a Certification Authority, and where the signing of the second system generated certificate is by hashing at least some data in the certificate to obtain a hash value, encrypting this hash value using the private key of the first system private-public key pair, and adding the encrypted hash value to the certificate.

9. *(original)* A method as defined in claim 8, wherein the private key of first system private-public key pair is stored in a wireless identity module.

10. *(original)* A method as defined in claim 9, wherein the private key of the first system is accessed by entry of a password.

11. *(original)* A method as defined in claim 6, where the identity of the user in the first system comprises a private-public key pair and an associated certificate issued by a Certification Authority.

12. *(original)* A method as defined in claim 11, wherein the private key of first system private-public key pair is stored in a wireless identity module.

13. *(original)* A method as defined in claim 12, wherein the private key of the first system is accessed by entry of a password.

14. *(original)* A method as defined in claim 1, wherein the authenticated identity of the user of the first system forming at least part of the signing of the certificate for the key for use in the second system includes encryption of data with the private key of the user of the first system, wherein the identity of the user of the first system is certified by a Certification Authority through a corresponding public key for the user of the first system.

15. *(original)* A method as defined in claim 14, wherein prior to signing the certificate for the key for use in the second system, the user of the first system obtains access to its private key by entry of a password.

16. *(original)* A method as defined in claim 15, wherein the password is a personal identification number.

17. *(original)* A method as defined in claim 1, wherein the certificate for the key includes the full certification tree for the key, said full certification tree including a certificate of the first system for the user of the first system.

18. *(original)* A method as defined in claim 1, wherein the first system is a wireless communication system.

19. *(original)* A method as defined in claim 18, wherein the second system a computer connected to the Internet.

20. *(original)* A method as defined in claim 17, wherein the second system uses a security protocol for establishing a secure session.

21. *(original)* A method as defined in claim 20, wherein the security protocol is selected from the group consisting of Transport Layer Security, IP Security Protocol and Secure Socket Layer.

22. *(original)* A method as defined in claim 20, wherein the wireless communication system uses a wireless identity module (WIM) in an associated wireless device of the user of the first system for establishing the identity of the user of the first system.

23. *(original)* A method as defined in claim 22, wherein the WIM contains a private key of the user of the first system and wherein a corresponding public key of the user of the first system is certified by a Certification Authority.

24. *(original)* A method as defined in claim 1, wherein the certificate for the key for use in the second system contains one or more usage limitations.

25. *(original)* A method as defined in claim 24, wherein one usage limitation is that a third party of the second system should accept the key for use in the second system only for certain types of operations.

26. *(original)* A method as defined in claim 25, wherein an accepted operation is the use of the key for use in the second system for encryption of data but not for signature verification.

27. *(original)* A method as defined in claim 1, where the certificate does not contain the identity of the user associated with the user generated key, and where the signing of the certificate using the authenticated identity of the user of the first system includes appending the full certification tree of the first user to the user generated key.

28. *(original)* A method as defined in claim 1, where the first and second users are the same entity.

29. *(currently amended)* A method of authenticating a user in a network environment where the user has an authenticated identity not associated with said network environment, comprising ~~the steps of~~:

generating a key for use in the network environment;

generating a certificate for the key; and

establishing the identity of the user in said network environment by signing the certificate for the key using the user's authentica ted identity.

30. *(currently amended)* A system for authenticating a user of a second system where the user has an authenticated identity in a first system, comprising:

a device forming part of the second system, the device having means for causing a key to be generated for use in the second system,

said device of the second system having means for generating a certificate for the key; and

a second device forming part of the first system, the second device having means for storing information regarding the authenticated identity of the user in the first system,

said second device further having means for communicating said information; and

wherein the device of the second system has means for receipt of said information from the second device, and further has means for establishing the identity of the user in the second system by signing the certificate for the key using the authenticated identity of the user in the first system.

31. *(original)* A system as defined in claim 30, wherein the device of the second system further comprises means for generating said key.

32. *(original)* A system as defined in claim 30, wherein the second device forming part of the first system further comprises means for generating said key.

33. *(original)* A system as defined in claim 30, wherein a third party communicates with the user of the second system, said third party communicating via a third device, said third device having means for verifying the user of the second system by the authenticated identity of the user of the first system.

34. *(original)* A system as defined in claim 33, wherein the third device is a server.

35. *(original)* A system as defined in claim 30, wherein the key comprises a private-public key pair and where the certificate includes the public key of the key pair.

36. *(original)* A system as defined in claim 35, wherein the certificate further includes an identity which is the same as the authenticated identity of the user of the first system.

37. *(original)* A system as defined in claim 36, where the authenticated identity of the user in the first system comprises a private-public key pair and a certificate issued by a Certification Authority, and where the means for signing the second system generated certificate is by encrypting this second system generated certificate using the private key of the first system private-public key pair.

38. *(original)* A system as defined in claim 37, wherein the private key of the first system private-public key pair is stored in a wireless identity module forming part of the second device.

39. *(original)* A system as defined in claim 38, wherein the second device includes means for user entry of information, wherein the private key of the first system is accessed by entry of a password via said user entry means.

40. *(original)* A system as defined in claim 35, where the identity of the user in the first system comprises a private-public key pair and an associated certificate issued by a Certification Authority.

41. *(original)* A system as defined in claim 40, wherein the private key of the first system private-public key pair is stored in a wireless identity module forming part of the second device.

42. *(original)* A system as defined in claim 41, wherein the private key of the first system is accessed by entry of a password.

43. *(original)* A system as defined in claim 30, where the user of the first system authenticated identity includes a private-public key pair, where the identity of the user of the first system is certified by a Certification Authority through a corresponding public key for the user of the first system, and wherein the means for signing the certificate includes signing the certificate for the key for use in the second system by encryption of data with the private key of the user of the first system.

44. *(original)* A system as defined in claim 43, wherein the second device includes means for user entry of information, and wherein the user of the first system obtains access to its private key by entry of a password via said user entry means.

45. *(original)* A system as defined in claim 44, wherein the password is a personal identification number.

46. *(original)* A system as defined in claim 30, wherein the certificate for the key includes the full certification tree for the key, said full certification tree including a certificate of the first system for the user of the first system.

47. *(original)* A system as defined in claim 30, wherein the first system is a wireless communication system.

48. *(original)* A system as defined in claim 47, wherein the second system is a computer connected to the Internet.

49. *(original)* A system as defined in claim 44, wherein the second system uses a security protocol for establishing a secure session.

50. *(original)* A system as defined in claim 49, wherein the security protocol is selected from the group consisting of Transport Layer Security, IP Security Protocol and Secure Socket Layer.

51. *(original)* A system as defined in claim 49, wherein the second device forming part of the wireless communication system includes a wireless identity module (WIM) for storing information used to establish the identity of the user of the first system.

52. *(original)* A system as defined in claim 51, wherein the WIM contains a private key of the user of the first system and wherein a corresponding public key of the user of the first system is certified by a Certification Authority.

53. *(original)* A system as defined in claim 30, wherein the certificate for the key for use in the second system contains one or more usage limitations.

54. *(original)* A system as defined in claim 53, wherein one usage limitation is that a third party of the second system should accept the key for use in the second system only for certain types of operations.

55. *(original)* A system as defined in claim 54, wherein an accepted operation is the use of the key for use in the second system for encryption of data but not for signature verification.

56. *(previously presented)* A system as defined in claim 30, where the certificate does not contain the identity of the user associated with the user generated key, and where the means for signing of the certificate using the authenticated identity of the user of the first system including appending the full certification tree of the first user to the user generated key.

57. *(original)* A system as defined in claim 30, where the first and second users are the same entity.

58. *(previously presented)* A system for authenticating a user in a network environment where the user has an authenticated identity not associated with said network environment, the system comprising:

means for generating a certificate for a key in the network environment; and

means for establishing the identity of the user in said network environment by signing the certificate for the key using the user's authe nticated identity.

59. *(currently amended)* A device for authenticating a user of a second system where the user has an authenticated identity in a first system, wherein the device forms part of the second system comprising:

means for generating a key for use in the second system;

means for generating a certificate for the key;

means for transferring the certificate to a device forming part of the first system, said device of the first system having information concerning the authenticated identity of the user in the first system, so as to establish the identity of the user in the second system by signing the ~~sign the~~ certificate using the authenticated identity of the user in the first system; and

wherein said device of the second system further comprises means for receipt of said signed certificate and means for transferring the signed certificate to a third party of said second system.

60. *(currently amended)* A wireless device for use in authenticating a user of a second system where the user has an authenticated identity in a first system associated with the wireless device, wherein the second system includes a device having means for causing a key to be generated for use in the second system, means for generating a certificate for the key, and means for transferring the certificate to another device;

wherein the wireless device comprises:

means for storing information regarding the authenticated identity of the user in the first system;

means for receipt of the certificate from the second device; and

means for establishing the identity of the user in the second system by signing the certificate using the authenticated identity of the user in the first system and transferring the signed certificate to the device of the second system.

61. *(original)* A wireless device as defined in claim 60, wherein the second device includes means for generating the key to be used in said second system.

62. *(original)* A wireless device as defined in claim 56, wherein the wireless device further comprises means for generating the key to be used in the second system.

63. *(original)* A wireless device as defined in claim 60, where the authenticated identity of the user in the first system comprises a private-public key pair and a certificate issued by a Certification Authority, and where the means for signing the second system generated certificate is by encrypting this second system generated certificate using the private key of the first system private-public key pair, wherein the wireless device includes a wireless identity module for storing said private key of the first system private-public key pair.

64. *(original)* A wireless device as defined in claim 63, wherein the wireless device includes means for user entry of information, wherein the private key of the first system is accessed by entry of a password via said user entry means.

65. *(currently amended)* A program stored on a computer readable medium for execution by a processor, for implementing the authentication of a user of a second system where the user has an authenticated identity in a first system, further comprising:

a device forming part of the second system, the device having program code stored in said computer readable medium for generating a key for use in the second system,

said device of the second system having program code stored in said computer readable medium for generating a certificate for the key; and

a second device forming part of the first system, the second device having program code stored in said computer readable medium for storing the authenticated identity of the user in the first system; and

wherein the second device has program code stored in said computer readable medium for establishing the identity of the user in the second system by signing the certificate generated by the device of the second system using the information regarding the authenticated identity of the user in the first system and transferring the signed certificate to the device of the second system.